Key Distribution via a Memory Device

ABSTRACT OF THE DISCLOSURE

An encryption system prevents a replay attack by providing a secure item that is substantially unique for each recording of copy-protected content material. A memory element is provided in the recording medium that is readable but not writeable by external devices, and whose content changes each time select material is recorded onto the medium. In a preferred embodiment, the content of this memory element is used to form a unique encryption key that is used to encrypt the content encryption key. This unique encryption of the content encryption key is further encrypted using a public key that corresponds to a private key of the intended rendering device. Although the unique encryption key is determinable by reading and processing the content of the externally read-only memory element, the decryption of the content encryption key requires both the unique encryption key and the private key of the intended rendering device. Because the unique encryption key is based on a content value of the read-only memory element that is unique to each recording to the recording medium, a subsequent illicit re-recording of the original encrypted content material onto the recording medium (a replay attack) will not provide the same unique encryption key as the unique encryption key used to originally encrypt the content encryption key. Because the unique encryption key of the replay attack differs from the original unique encryption key used to encrypt the content encryption key, the rendering device will be unable to decrypt the content encryption key, and thereby will be unable to decrypt the content material, and the replay attack will fail.